UNITED STATES DISTRICT COURT

DISTRICT OF SOUTH DAKOTA

SOUTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. ROBERT JOHN HULSCHER, Defendant.	4:16-CR-40070-01-KES REPORT & RECOMMENDATION

INTRODUCTION

Defendant Robert John Hulscher is before the court pursuant to a superseding indictment charging him with stealing 12 firearms and aiding and abetting the theft of those firearms, and with being a felon in possession of the same 12 firearms, in violation of 18 U.S.C. §§ 922(g)(1), and 924(l) and 2. See Docket No. 242. Mr. Hulscher has moved to suppress certain evidence the United States obtained without a warrant from a copy of digital information extracted from his cell phone in an unrelated state court prosecution. See Docket No. 223. The government opposes the motion. See Docket No. 232. This matter was referred to this magistrate judge to hold an evidentiary hearing and to make findings of fact and a recommended disposition pursuant to 28 U.S.C. § 636(b)(1)(B) and the October 16, 2014, standing order of the Honorable Karen E. Schreier, district judge.

FACTS

An evidentiary hearing was held on Mr. Hulscher's motion on February 7, 2017. Mr. Hulscher was present in person with his counsel. The government was represented through its Assistant United States Attorneys. No witnesses testified at the hearing but 11 exhibits were received, five from the government and six from Mr. Hulscher. In addition, the parties stipulated that the court could take judicial notice of the exhibits submitted before the district court in the motion to exclude, specifically the document filed at the court's Docket No. 208-3 and Defendant's Exhibit 5 from the January 27, 2017, hearing. From this evidence the court makes the following findings of fact.

Police in Huron, South Dakota investigated Mr. Hulscher for forgery, counterfeiting, and identity theft charges beginning on March 15, 2016, when Mr. Hulscher attempted to cash a forged check at a Huron business and then fled the premises before completing the transaction. As part of their investigation of Mr. Hulscher, the Huron police obtained a search warrant to search and seize any evidence on Mr. Hulscher's cell phone related to the state court charges of forgery, counterfeiting, and identity theft. See Exhibit 2.

The affidavit in support of that search warrant set forth the fact that on March 15, 2016, Huron Police Sergeant Mark Johnson arrived at a Huron business and observed a red Chevy pickup on the north side of the business. See Exhibit 1 at 3. A male exited the business, entered the pickup, and drove off. Id. Sgt. Johnson made contact with the owner of the business who informed Sgt. Johnson the male who left in the red pickup was the one who

tried to cash a suspicious check. Id. Sgt. Johnson pursued the red pickup and effected a traffic stop. Id. Mr. Hulscher identified himself to Sgt. Johnson and acknowledged he was trying to cash a forged check at the business. Id. Mr. Hulscher said he was doing so at the insistence of a female named Nikki, who used to live in Huron. Id. Mr. Hulscher explained he owed Nikki money for illegal drugs and cashing the forged check was an attempt to obtain the money necessary to repay Nikki. Id. at 3-4. Mr. Hulscher admitted prior drug use. Id. at 3. Mr. Hulscher reported that Nikki had threatened him, phoned him repeatedly, and damaged his vehicle in connection with the drug debt he owed. Id. at 3-4. Mr. Hulscher was detained by Sgt. Johnson on suspicion of forgery and transported to the Huron police department. Id. at 4.

At the police department, Detective Gene Miller interviewed Mr. Hulscher in the presence of Sgt. Johnson. Id. After being advised of his Miranda[1] rights and waiving those rights, Mr. Hulscher reiterated much of the information he had previously told to Sgt. Johnson at the scene of the traffic stop. Id. at 4-5. The officers tried to obtain more information about Nikki, but were unsuccessful. Id. at 5. The officers asked for consent to search Mr. Hulscher's cellular phone, but ultimately, Mr. Hulscher refused to consent. Id. Sgt. Johnson then seized Mr. Hulscher's phone and explained to him that the officers would be seeking a search warrant for it. Id. While Sgt. Johnson was in possession of the phone, a text message appeared from a male asking "You

[1] Miranda v. Arizona, 384 U.S. 436 (1966).

holdin?" Id. Mr. Hulscher was then arrested and transported to the Beadle County Correctional Center. Id.

Sgt. Johnson told the issuing judge in his search warrant affidavit that, in his training and experience, persons involved in counterfeiting operations typically carry cell phones, that those phones contain names and phone numbers of customers and suppliers, and that text messages, audio memos, videos, and photographs are typically stored in the internal memory of cell phones and often used for communication with drug distributors and customers. Id. Sgt. Johnson stated Mr. Hulscher possessed multiple counterfeit checks and multiple counterfeit identification cards. Id. at 6. Sgt. Johnson then stated: ***"I request permission to enter the cell phone to collect any evidentiary information regarding this counterfeit investigation."*** Id. (emphasis supplied). Sgt. Johnson then explained the method of search: the phone would be seized and processed by a computer specialist in an appropriate setting. Id. Sgt. Johnson requested permission to seize the phone, to conduct an offsite examination of it, and to transport the phone to a facility for such analysis. Id.

A state court judge issued the search warrant on March 16, 2016. See Exhibit 2. The warrant authorized police to search Mr. Hulscher's cell phone as well as a Verizon wireless tablet discovered in Mr. Hulscher's pickup truck.[2] The warrant allowed a search for "property that constitutes evidence of the commission of a criminal offense," "contraband, the fruits of crime, or things

[2] Mr. Hulscher had given police consent to search his truck at the scene of the traffic stop.

otherwise criminally possessed," and "property designed or intended for use in, or which is or has been used as the means of, committing a criminal offense." Id. at 1. The warrant went on to state police were "commanded to search" the phone and the tablet "for the following property (describe with particularity):"

1. The content of any texts, including but not limited to incoming texts, sent texts, draft texts and deleted texts that were sent or received by the cellular communication devices.
2. Incoming or outgoing cell phone call records by the cellular communication devices.
3. The content of the address book for the cellular communication devices.
4. Video and/or photgraphs on the phones [sic] or stored in the internal memory of the cellular communication devices.
5. Any other data on the communication device ***as it relates to this case.***

See Exhibit 2 at 2 (emphasis supplied). The state court search warrant required police to conduct the requested search within 10 days. Id.

As part of the procedure used by the police in executing this search warrant, Detective Casey Spinsby of the Huron Police Department extracted digital information from the phone on April 11, 2016, making a copy of that digital data. See Exhibit A at 7. Det. Spinsby then reported what he found in his examination of the digital data extracted from Mr. Hulscher's cell phone. Id. at 8-9.

Det. Spinsby noted several examples of evidence relevant to Mr. Hulscher's fraud, forgery, and identity theft charges. Id. In addition, Det. Spinsby noted 531 messages on Mr. Hulscher's cell phone related to the sale, use, or purchase of illegal drugs. Id. at 8-9. Other than drugs and forgery, Det. Spinsby stated he ***"did not locate any other data or files with***

evidentiary value in the extractions." Id. at 9 (emphasis supplied). In other words, Det. Spinsby found nothing of note with regard to firearms offenses involving Mr. Hulscher. Following his review of the entirety of the data on Mr. Hulscher's phone (see Exhibit 5), Det. Spinsby segregated the data on the phone that was relevant to the Huron state court prosecution and saved that data separately. See Exhibit F.

The state court charges against Mr. Hulscher were resolved on May 17, 2016, when Mr. Hulscher was sentenced for those offenses after having previously entered a plea of guilty to grand theft. See Exhibit B. Mr. Hulscher did not appeal his sentence or conviction. On May 20, 2016, the state dismissed the other charges in the complaint previously asserted against Mr. Hulscher to which he did not plead guilty. See Exhibit C.

On May 17, 2016, the date of Mr. Hulscher's sentencing in state court on the counterfeit/forgery/theft charges, Jennifer Hulscher made an application to the state for return of Mr. Hulscher's cell phone and tablet for the reason that his case had been resolved. See Exhibit D. The state court judge issued an order on May 24, 2016, ordering Huron police to return Mr. Hulscher's cell phone and tablet back to Mr. Hulscher. See Exhibit 3. The Huron police returned the physical electronic devices to Mr. Hulscher's father, Jack Hulscher, but retained the copy of the digital information extracted from Mr. Hulscher's cell phone.

Mr. Hulscher alleges the government in this case knew about Mr. Hulscher's state court prosecution above-referenced at least as early as

April 19, 2016. However, they did not investigate the circumstances of the Huron case until January 12, 2017. See Exhibit E at 1-2; Docket No. 232 at 4. On January 12, 2017, Special Agent Brent Fair of the federal Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) contacted the Huron police and discovered the existence of the copy of the digital information extracted from Mr. Hulscher's phone. Id. He requested that copy be sent to him and received via mail a DVD disc which contained a partial copy of the phone data—this was the data Det. Spinsby had previously segregated and which was relevant to the state court prosecution. See Docket No. 232 at 4; Exhibit F. Agent Fair contacted the Huron Police Department the same day to find out if a complete copy of the digital data from Mr. Hulscher's phone existed and found out it did. See Docket No. 232 at 4.

On January 18, 2017, Agent Fair physically traveled to Huron, South Dakota, along with Special ATF Agent Kevin Wiese, and obtained this complete digital copy from the Huron police. See Exhibit E at 2; Exhibit 5. Without first obtaining a search warrant to search for evidence of firearms offenses, Agent Fair began searching through the data from Mr. Hulscher's phone while the two ATF agents were still en route back to Sioux Falls, South Dakota. Id. Agent Fair found evidence relevant to this federal firearms prosecution that Mr. Hulscher and co-defendant Nicholas Hemsher had contact with each other via cell phones from January 10, 2016, through February 22, 2016. Id. Agent Fair also found it relevant that Mr. Hulscher apparently deleted Mr. Hemsher's contact information from his phone on February 22, 2016, at 1:23:48 p.m. Id.

The superseding indictment in this case alleges Mr. Hulscher committed his firearms offenses between February 18 and 22, 2016. See Docket No. 181. Finally, Agent Fair found the content of various communications on the phone to indicate Mr. Hulscher's possible motives for committing the firearms offenses with which he is charged in this federal case (lack of funds, drug use). Id. at 4.

Mr. Hulscher argues that Agent Fair's warrantless search of the digital information extracted from his phone by the Huron police violates his Fourth Amendment right to be free from unreasonable searches and seizures in three ways: (1) the retention by the Huron police department of the digital copy of the information from Mr. Hulscher's cell phone violated his rights, (2) the search by Agent Fair was conducted after the 10-day period allowed by the state court search warrant, and (3) the search by Agent Fair was not authorized by the state court search warrant because Agent Fair was searching for evidence of firearms offenses while the state warrant authorized a search for evidence of forgery, counterfeiting, and identity theft. Mr. Hulscher further argues (4) that no exception to the warrant requirement is applicable to Agent Fair's warrantless search.

The government characterizes Agent Fair's search as being conducted pursuant to the earlier state court search warrant and, since that warrant was validly issued, argues that Agent Fair's search complied with the Fourth Amendment. Alternatively, the government argues that Agent Fair's search was authorized by the state court warrant and, even if that warrant was invalid, Agent Fair relied in good faith on the warrant. The government also

argues Mr. Hulscher has no privacy interest in the digital data Agent Fair searched. Finally, the government argues the evidence was lawfully obtained under the plain view doctrine.

DISCUSSION

A. Fourth Amendment Law

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

The touchstone of the Fourth Amendment is "reasonableness," and "reasonableness" usually requires the government to obtain a search warrant before searching for evidence of a crime. Riley v. California, 573 U.S. ___, 134 S. Ct. 2473, 2482 (2014). Without a warrant, a search is "reasonable" only if it fits into a specific exception to the warrant requirement. Id. Whether to exempt a category of search from the warrant requirement is determined by weighing "the degree to which [the search] intrudes upon an individual's privacy and," "the degree to which it is needed for the promotion of legitimate governmental interests." Id. at 2484. Where a search takes place without a warrant, it is the government's burden to demonstrate by a preponderance of the evidence that an exception to the warrant requirement applies. Coolidge v. New Hampshire, 403 U.S. 443 (1971); United States v. Kennedy, 427 F.3d 1136, 1140 (8th Cir. 2005).

The chief evil which the Fourth Amendment was intended to address was the hated "general warrant" of the British crown. Payton v. New York, 445 U.S. 573, 583-84 (1980). General warrants gave British officials "blanket authority to search where they pleased" for evidence of law violations. Id. at 583 n. 21; Ashcroft v. al-Kidd, 563 U.S. 731, 742 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown"). The problem posed by general warrants is "of a general, exploratory rummaging in a person's belongings." Andresen v. Maryland, 427 U.S. 463, 480 (1976).

The Fourth Amendment redresses the general warrant with its requirement that the thing to be searched for and seized must be stated with particularity (the particularity requirement). Id. The particularity requirement not only prevents the issuance of general warrants, it also "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." Groh v. Ramirez, 540 U.S. 551, 561 (2004); al-Kidd, 563 U.S. at 742-43 ("[t]he principal evil of the general warrant was addressed by the Fourth Amendment's particularity requirement"). The particularity requirement "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Andresen, 427 U.S. at 480.

"In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . responsible officials, including judicial officials, must take care to assure that [such searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy." Andresen, 427 U.S. at 482 n.11. If officials find they have overseized documents by taking documents not within the scope of the search warrant (nonresponsive documents), police should return those documents and the court should suppress them if not returned. Id. See also United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982) (holding government's wholesale seizure of documents and taking them back to headquarters to sort through and find what was specified in the search warrant, as well as government's refusal to return nonresponsive documents, was of doubtful legality under the Fourth Amendment).

If one were to apply precedent from the analog age to modern practices of obtaining digital evidence, today's current practices would not pass constitutional muster. That is because the most common practice when dealing with digital evidence is for police to make an electronic copy of all of the digital data on an electronic device and then take that copy back to headquarters and search through it at their leisure. See FED. R. CRIM. P.

41(e)(2)(B) (acknowledging that search of electronic data will take place in a two-step process).[3]

The Supreme Court has recognized its past Fourth Amendment precedent dealing with searches of physical items and paper documents may not strike the appropriate balance when applied to digital evidence. Riley, 134 S. Ct. at 2485; United States v. Jones, 565 U.S. 400 (2012). In the case of GPS monitoring of a suspect's car for a month, the electronic data disclosed by the GPS device will reflect "a wealth of detail about [the suspect's] familial, professional, religious, and sexual associations" that police might store and mine for years into the future, with little or no inconvenience or cost. Jones, 565 U.S. at 955-56 (Sotomayer, J., concurring). Furthermore, such electronic surveillance surpasses the data that traditionally could be gained when police physically "tailed" a car themselves while, at the same time, "evad[ing] the ordinary checks that constrain abusive law enforcement practices." Id. at 956.

Likewise, the ease and inexpense with which police can seize and copy entire hard drives, whether of a computer or a cell phone, allows police to quickly and cheaply obtain hundreds and thousands of discrete, disparate chunks of data about all of a person's areas of her life. Riley, 134 S. Ct. at 2489. Just as with GPS data, that data can be stored and mined for years into

[3] South Dakota law appears not to reflect the modern reality of electronic searches as the law still provides for a 10-day search period and does not acknowledge any two-step process. See SDCL § 23A-35-4. The court need not address this issue as Mr. Hulscher stated at oral argument at the evidentiary hearing in this matter that he was taking no issue with the validity of the state court search warrant or the method in which Huron police executed that search warrant—as concerns the state court forgery/counterfeiting/identity theft prosecution.

the future, resembling for all the world the hated British crown's general warrants.

Courts have grappled with the problem of applying Fourth Amendment analysis to searches of electronic/digital data. Efforts to limit searches of digital information or to limit seizures of digital information at the inception of a search by, for example, using search terms, have met with little success. Computer users may "name, rename, and store files in ways that allow the 'files containing evidence of a crime [to] be intermingled with millions of innocuous files.' " United States v. Morgan, 562 Fed. Appx. 123, 128 (3d Cir. 2014) (quoting United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013)). Thus, it is unavailing to try to devise limits on how a search of digital data may be conducted or what may be seized by specifying to search only in directories or files of a certain name or type. Id.

Thus, the practice has evolved that, on the issuing end of a search warrant, courts have given police broad latitude in what is searched and seized, usually allowing police to copy entire hard drives, so long as the object of the search is adequately set forth in the search warrant. See e.g. Morgan, 562 Fed. Appx. at 128; United States v. Galpin, 720 F.3d at 447; United States v. Richards, 659 F.3d 527, 537-38 (6th Cir. 2011); United States v. Comprehensive Drug Testing, Inc. (CDT), 621 F.3d 1162, 1176 (9th Cir. 2010) (*en banc, per curiam*). This eventuality at the gathering stage came about through necessity: the nature of the technology itself dictates the method. See

Orin S. Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, 48 Tex. Tech. L. Rev. 1 (2015).

But because of the very breadth given the seizure of electronic data on the front end, police and courts know the seizure will in all reality contain a great deal—perhaps the overwhelming majority—of data which is nonresponsive to the reasons giving rise to probable cause for the search warrant in the first place. The question becomes what to do about that vast quantity of digital information which is *not* covered by the scope stated with particularity in the search warrant.

This problem is magnified by the breathtaking depth and scope of digital evidence each of us has on our computers and on our cell phones. "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." Riley, 134 S. Ct. at 2489. Calling these items a phone or a computer is a misnomer as they may just as aptly be called a library, a camera, a tape recorder, a video player, a rolodex, a diary, an album, a newspaper, or a tv. Id. Current cell phones can store millions of pages of text, thousands of photographs, and hundreds of videos. Id. They can also store information of many different types—financial, health, mental impressions. Id. Cell phones, by amalgamating a variety of discrete data about the owner all in a single place, have the potential to invade the owner's privacy to a degree that could not be possible if just one variety of data were discovered. Id. Thus, the nature of digital data technology requires it be overseized in the initial phase of a search, but carries with it the potential

for invasion of privacy of several degrees of magnitude greater than has ever been possible in the past. How to apply the Fourth Amendment to this conundrum is the issue before this court.

The Riley decision itself is of great help. That decision establishes the rule that, generally, police must obtain a search warrant before searching a cell phone and may not regularly rely upon the exception to the warrant requirement for warrantless searches incident to arrest. Riley, 134 S. Ct. at 2494-95. This opinion addresses a related question: what rules govern the government's search of the overseized nonresponsive digital cell phone data outside the scope of the warrant once obtained?

1. There Were Two Searches, Not One

The court first addresses the idea implicit in the government's arguments against suppression: that ATF Agent Fair's search on January 18, 2017, was pursuant to the state court search warrant issued on March 16, 2016, to the Huron police department. The court rejects this contention. First, the government introduced no evidence that Agent Fair even knew of the prior state court search warrant when he conducted his search. Agent Fair did not testify nor did Det. Spinsby. All that is recounted in Agent Fair's reports is that he learned of the existence of the digital copy of Mr. Hulscher's phone and requested a copy for use in his federal firearms investigation. See Exhibit E. Thus, Agent Fair cannot be said to have acted pursuant to a search warrant of which there is no evidence he was aware.

The government argues the state court search warrant authorizes a search of Mr. Hulscher's cell phone for evidence of *any* crime and that this, then, is a broad enough formulation to cover Agent Fair's search for evidence of firearms crimes. The court rejects this argument too. Although the face of the warrant allows a search seemingly as broad as the government asserts, this assertion runs into two problems. If the warrant were truly as broad as government counsel interprets it for purposes of Agent Fair's search, it would in fact be a "general warrant" and would be invalid on that basis. Al-Kidd, 563 U.S. at 742; Payton, 445 U.S. at 583 n.21; Andresen, 427 U.S. at 480.

This, of course, is not true. The broad initial language of the search warrant is modified and restricted by the passages that follow on pages 1-2 of the warrant. Those passages authorize the search of Mr. Hulscher's phone for texts, phone call records, contacts, videos and photographs ***"as it relates to this case."*** See Exhibit 2 at 2. Clearly, interpreting the warrant in light of the affidavit submitted in support of the request for the warrant, "this case," means the forgery/counterfeiting/identity theft case for which Mr. Hulscher was then being investigated. One might even interpret the search warrant to authorize the Huron police to search for evidence of drug trafficking, since that was mentioned in the affidavit too. See Exhibit 1. However, the original warrant clearly did not authorize the Huron police to search for evidence of firearms offenses. See Exhibits 1 & 2. The search for evidence of firearms offenses was a separate, second, search and it was not conducted pursuant to the original state court warrant.

2. Mr. Hulscher Has a Recognized Privacy Interest

Fourth Amendment protections apply only where (1) the person subject to a search or seizure had a subjective expectation of privacy in the thing seized or place searched and (2) that expectation of privacy was one that society accepted as objectively reasonable. California v. Greenwood, 486 U.S. 35, 39 (1988). The government argues that once the state court search warrant was issued, Mr. Hulscher no longer had an expectation of privacy in the contents of his phone that society would accept as objectively reasonable.

Again, if there were but one search that had occurred in this case, the court would agree with the government's contention. As to the search conducted by Det. Spinsby pursuant to the search warrant issued by the state court judge in connection with the forgery/counterfeiting/identity theft investigation, the court agrees Mr. Hulscher had no expectation of privacy in the data on his phone *as to that search* that society would recognize as objectively reasonable. The search warrant was lawfully applied for and issued. Mr. Hulscher has stated in this suppression motion he takes no issue with how the state court search warrant was obtained or executed—as to the state court search.

But as the court has already concluded, Agent Fair's search was not conducted pursuant to the state court search warrant. Instead, it was a subsequent warrantless search conducted for a different purpose entirely. Mr. Hulscher had a privacy interest in the digital data on his cell phone. Riley, 134 S. Ct. at 2493. That privacy interest was one that society recognizes as

objectively reasonable. Id. Furthermore, the court notes that, intervening between the first search by Det. Spinsby pursuant to warrant, and the second warrantless search by Agent Fair, Mr. Hulscher had requested the Huron police department to return his phone to him and the state court judge had granted that request. See Exhibits D & 3. If Mr. Hulscher could be said to have been divested of a reasonable expectation of privacy in his phone due to the issuance of the state court search warrant on March 16, 2016, that privacy interest reattached once the state court judge ordered his phone to be returned to him on May 24, 2016. Agent Fair came into possession of the digital data on Mr. Hulscher's phone some seven and one-half months later.

The government orally argued further that, once Mr. Hulscher lost the reasonable expectation of privacy in his phone through issuance of the state court search warrant, that expectation of privacy never reattaches. The government cites to no authority that establishes this proposition. Furthermore, the court is aware of none. It is not the law that once a place is searched pursuant to a valid warrant, the person who owns the property searched can never again regain his or her privacy. If that were the law, any home which had—in the past—been subject to a valid search warrant could be continually searched again and again by police at any time stretching into the future because there would never again be a reasonable expectation of privacy. That is simply not the law. The court holds that Mr. Hulscher had a reasonable expectation of privacy in the information from his cell phone once the state court judge ordered the Huron police to return his phone to him.

3. Leon Good Faith Exception Does Not Apply

The government asserts Agent Fair's search of Mr. Hulscher's digital phone data should not be excluded from evidence in this case because he relied in good faith on the state court search warrant. This requires the court to indulge the government's theory that Agent Fair's search was pursuant to that state court warrant, an indulgence in which the court is unwilling to engage.

As the government itself admits, "the exclusionary rule does not apply 'when an officer acting with objective good faith *has obtained a search warrant* from a judge or magistrate and *acted within its scope*.' " See Docket No. 232 at 13 (citing United States v. Houston, 665 F.3d 991, 994 (8th Cir. 2012)) (emphasis added). Here, Agent Fair obtained no search warrant, there is no evidence he even knew of the earlier warrant, and he was clearly not acting within the scope of that warrant.

If an affidavit in support of a search warrant fails to provide probable cause for the issuance of the search warrant, the fruits of the search will not be suppressed if the officer who executed the search warrant relied upon that warrant in objective good faith. United States v. Ross, 487 F.3d 1120, 1122-1123 (8th Cir. 2007) (describing Leon good-faith exception and citing United States v. Leon, 468 U.S. 897, 921, (1984)). "When assessing the good faith of the officers, [the court] look[s] to the totality of the circumstances, including any information known to the officers, but not included in the affidavit." United States v. Rodriguez, 484 F.3d 1006, 1011 (8th Cir. 2007). The question is whether a reasonably well-trained officer would have known that the search

was illegal despite the issuing judge's authorization. United States v. Hudspeth, 525 F.3d 667, 676 (8th Cir. 2008).

Here, the government introduced no evidence that Agent Fair was aware of the state court search warrant. In addition, he was clearly not executing the first search warrant when he conducted his search. Thus, the court cannot conclude that he relied on that warrant in good faith. Furthermore, had Agent Fair been given a copy of the search warrant, the court is confident he would have concluded—as the court does—that the warrant authorized police to search only for evidence of counterfeiting/forgery/identity theft and possibly drug offenses. The warrant did not authorize a search for evidence of firearms offenses. A reasonable officer who read the search warrant would have known that.

The government cites to the *en banc* decision in United States v. Ganias, 824 F.3d 199, 206 (2d Cir. 2016) (*en banc*), discussed in detail immediately below, holding that the Leon good-faith exception applied to the second search of the digital data in that case. Of course, the crucial fact necessary to the Second Circuit's analysis in Ganias was that the second officer who conducted the second search *obtained a second, valid search warrant* for her search, laying out for the issuing judge all the relevant facts. Id. at 207. Here, Agent Fair did not obtain a second search warrant for his subsequent search. Therefore, the holding in Ganias is inapplicable. Accordingly, the court concludes the government may not rely on Leon to avoid the exclusionary rule as to the fruits of Agent Fair's search.

B. Emerging Law on Digital Searches—United States v. Ganias

In Ganias, police in November, 2003, copied hard drives of computers belonging to Ganias, an accountant, in connection with an investigation of two of Ganias' clients who were suspected of defrauding the government. Ganias, 824 F.3d at 201. The search warrant authorized agents to seize all evidence relating to the business, finances and accounting operations of the two clients. Id. However, government agents made copies of *all* information on Ganias' computer hard drives, which included information about *all* of Ganias' clients and also included Ganias' personal financial records. Id. at 202-03.

Thirteen months after the copies were made of Ganias' computers, in December, 2004, investigators had finished their initial searching and seizing of relevant information from those copies, but the investigation of the two clients was, at this point, still ongoing. Id. at 206. Police did not purge or delete the non-responsive computer files at this time. Id.

In July, 2005, agents opened an investigation of Ganias himself. Id. at 207. Nine months into the investigation of Ganias, in April 2006, knowing that they still retained copies of Ganias' computer hard drives, police sought and received another search warrant to search the copies of Ganias' computer hard drives, this time seeking permission to search and seize evidence from Ganias' personal financial records. Id. The copies of Ganias' computer hard drives had been in the government's possession for two and one-half years at this point. Id.

Ganias was indicted for conspiracy and tax evasion and moved to suppress the fruits of the search of copies of his computer hard drives in the second search warrant. Id. at 207-08.

After an initial three-judge panel issued a decision, United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), rehearing *en banc* by the Second Circuit was subsequently granted. See United States v. Ganias, 791 F.3d 290 (2d Cir. 2015). The court instructed the parties to address (1) whether the practice of making a copy of a computer hard drive, retaining it indefinitely, and then subsequently searching the data again pursuant to a second search warrant violates the Fourth Amendment; and (2) whether the agents conducting the search acted in reasonable good faith. Id.

The *en banc* decision pointed out that, as of December 2004, although agents had searched through the computer copies for information about the two clients of Ganias, the investigations of those clients were still open and agents testified they did not want to delete the nonresponsive data at that point because to do so would alter the data seized. Ganias, 824 F.3d at 206. Instead, the agent testified the copies would have been released back to Ganias when the investigation was closed. Id. Additionally, the *en banc* opinion noted the agent who applied for the second search warrant for Ganias' personal information set forth the entirety of events that had occurred up to then, including the fact that the government had possessed personal computer files of Ganias for two and a half years, but had not accessed those files because the original search warrant did not authorize them to do so. Id. at 207.

The district court in Ganias' case had concluded the officers did not violate Ganias' Fourth Amendment rights, so the court never addressed the Leon good faith exception. Id. at 209. The Second Circuit in its *en banc* decision concluded the officers acted with objective good faith, so that court never reached the question whether a Fourth Amendment violation occurred. Id. Nevertheless, it offered guidance (*dicta*) for the future for searches in this significant and complex Fourth Amendment context. Id.

Ganias relied on a Ninth Circuit case involving an overly broad seizure of physical paper documents by police, which they transported back to their headquarters and sorted by relevance. Id. (citing Tamura, 694 F.2d 591). The Ninth Circuit had held the overbroad seizure and the subsequent retention of irrelevant documents violated the Fourth Amendment. Id. at 210-11 (citing Tamura, 694 F.2d at 595, 597).

The Ganias court held Tamura was not analogous to computer files. Id. at 211. Computer files are not like paper files in that they are not stored in a discrete physical location; they are "fragmented" on a storage device, potentially in various physical locations separate and distinct from other files. Id. at 213. Because of this, it is often not possible to fully extract or segregate responsive digital data from non-responsive digital data on a storage device without altering the evidence. Id. at 213, 215. Furthermore, the government may seek to prove that something *did not* exist on the digital storage medium, as when a defendant asserts a virus was responsible for placing something on his computer. Id. at 214. In such a case, it is necessary for the government to

examine the entire hard drive to confirm the virus is not there; examination cannot be limited in such a case to the areas of the storage device where relevant evidence resides. Id.

The record was incomplete in Ganias' case, with no information about the significant privacy concerns involved, or of the complex and rapidly evolving technology issues. Id. at 220-21. Therefore, the court declined to address the question whether the government's retention of the mirror images of Ganias' computer hard drives violated the Fourth Amendment. Id. Instead, the court held the agents in Ganias' case had acted with objectively good faith reliance on the second search warrant that was obtained because the officers disclosed to the judge issuing the second search warrant all crucial facts relative to the search request and the officer had no significant reason to believe he had acted unconstitutionally. Id. at 221-25.

Two things are relevant to Mr. Hulscher's case from the Ganias opinion. First, the agents in Ganias seeking to search the digital data previously copied years earlier sought a second search warrant, as Agent Fair in this case did not. It was appropriate for the agents in Ganias to obtain a second search warrant because the data they wanted to search for (information about Ganias' own culpability) was separate and distinct from the scope of the information the first search warrant authorized the agents to search for (evidence of the Ganias' clients' culpability).

A second observation from Ganias is that there was nothing in the record—just as there is nothing in this record—indicating the first agents

executing the first search warrant observed obviously incriminating information about the subject matter of the second search. In Ganias, the second subject matter was Ganias' own culpability; here it is Mr. Hulscher's culpability for firearms offenses, which was ***not*** noted by Det. Spinsby when he executed the first search warrant. Thus, it *cannot* be said that the evidence sought in the second search of the digital data in either case was in plain view of the officer who executed the first search warrant—in both cases, the first searcher made no note of the evidence sought in the second search.[4]

C. Plain View Doctrine

1. Plain View Should Not Be Applied to Digital Searches

The government asserts that Agent Fair's search of Mr. Hulscher's digital cell phone data can be justified under the plain view doctrine. The Court in Horton v. California, 496 U.S. 128 (1990), explained the plain view doctrine. Because *any* evidence seized by the police will likely be in plain view, the plain-view doctrine may only be used to justify a warrantless seizure when the initial intrusion that brings the police within plain view of the items seized is supported by one of the recognized exceptions to the warrant requirement.

[4] The Second Circuit in its *en banc* decision, in an effort to distinguish its conclusions from the earlier panel's decision, pointed out that the agent in Ganias who sought and obtained the second search warrant had developed probable cause through good old-fashioned gum-shoe detective work: the agent had examined Ganias' tax returns, subpoenaed his bank records, and looked for evidence of underreported income. Ganias, 824 F.3d at 206 n.14. Thus, through "paper" channels, the agent developed probable cause for the second search warrant independent of the retained mirror-image hard drives. Id. at 206-07, 207 n.15. Again, this is another way the Ganias case is different from this case. Agent Fair never sought to show independent probable cause for his search of the Huron digital data.

Horton, 496 U.S. at 135. The plain-view doctrine does not stand alone, rather it works in conjunction with a prior justification for the lawful presence of the police at the place of the warrantless seizure. Id. (citing Coolidge, 403 U.S. at 465-66). That is, a police officer who comes across evidence while in hot pursuit of a fleeing suspect, while validly arresting a defendant, or while executing a valid search warrant for other objects may rely on the plain view doctrine to seize items in plain view that are not covered by a warrant. Id. at 135-36 (citing Coolidge, 403 U.S. at 465-66). If a police officer has some legitimate reason for being present that is *unconnected* with a search directed against the defendant, that is, an officer is not searching for evidence against the accused, then any incriminating objects in plain view may be seized without a warrant. Id. at 135.

The plain view doctrine, in order to be applicable, requires that the police officer be lawfully in the place where s/he is when s/he views the evidence. Id. See also United States v. Morgan, 842 F.3d 1070, 1075 (8th Cir. 2016) (same). Also, the incriminating nature of the evidence must be immediately apparent to the officer. Horton, 496 U.S. at 142; United States v. Khabeer, 410 F.3d 477, 482 (8th Cir. 2005). Finally, the plain view doctrine requires the government to show the officer had a lawful right to access the object. Khabeer, 410 F.3d at 482.

The Ninth Circuit categorically rejected the "plain view" exception to the over-seizure of digital data in United States v. Comprehensive Drug Testing, Inc. (CDT), 621 F.3d 1162, 1170-71 (9th Cir. 2010) (*en banc, per curiam*). The

CDT case involved the government's investigation into the Bay Area Lab Cooperative (Balco), which was suspected of supplying professional baseball players with steroids. Id. at 1166. Major League Baseball (MLB) hired CDT to provide drug testing of *all* MLB players on an anonymous, confidential basis to see what percentage of players would test positive. Id. Federal authorities learned that 10 players had tested positive in the CDT program. Id.

The authorities then obtained a search warrant for a search of CDT's facilities; the warrant was limited to the records for the 10 players who had tested positive, the identities of whom were known to the government. Id. In executing the warrant, however, authorities seized electronic records for hundreds of MLB players as well as a great many other people not associated with MLB in any way. Id. Seizing agents then reviewed *all* the data seized and, on the basis of this nonresponsive data, sought and obtained subsequent search warrants in three other jurisdictions involving other MLB players. Id. at 1169.

As to the government's initial overseizure of data from CDT, the court accepted the government's contention that, because it could not be sure whether digital "data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file" on the computers, this required the government to seize the entire hard drive. Id. at 1170. The government then argued that once it seized the digital information from CDT and saw information showing steroid use by other baseball players aside from the 10 players listed in the original search warrant, that information was in

plain view and, thus, properly obtained by the government. Id. The very fact that the technology required the government to seize *all* electronic data in order to effectuate the limited search warrant was the exact feature that caused the Ninth Circuit to reject the plain view doctrine: if everything electronically seized by the government comes into plain view, it would create "a powerful incentive for them to seize more rather than less:" Why stop with one directory in a computer—just take the entire hard drive. Why stop with the hard drive on one computer—just make copies of the hard drive on all computers. "Let's take everything back to the lab, have a good look around and see what we might stumble upon." Id. at 1171. The application of the plain view doctrine to overseized electronic data would make a mockery of the Fourth Amendment's prohibition on general warrants. Id. at 1171, 1176. The government cannot be entitled to "keep anything one of its agents happened to see while performing a forensic analysis of a hard drive." Id. at 1171. See also United States v. Carey, 172 F.3d 1268, 1272-74 (10th Cir. 1999) (refusing to apply plain view doctrine to search for digital documents related to drug trafficking where police discovered evidence of child pornography and then actively abandoned the search for drug evidence and looked for more child pornography).

There is good reason not to apply the plain view doctrine to examinations of nonresponsive digital data that is not within the scope of the original warrant. When police make subsequent use of nonresponsive data, they are treating that data as though it was described within the scope of the original

search warrant—which it was not. See Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, 48 Tex. Tech. L. Rev. at 26. This eliminates the particularity requirement of the Fourth Amendment and "enables every computer warrant that is narrow in theory [or on paper] to become general in fact." Id.

"[T]he Fourth Amendment will not tolerate adoption of an overly broad categorical approach that would dilute the warrant requirement in a context where significant privacy interests are at stake." Missouri v. McNeely, 569 U.S. ___, 133 S. Ct. 1552, 1564 (2013). Digital evidence is, by necessity, routinely overseized. To adopt a "broad categorical approach" applying the plain view doctrine to digital evidence would likewise unreasonably dilute the warrant requirement. Id. Additionally, because of the breadth of the overseizure, significant privacy interests are at stake—often the great majority of the data seized (as in this case) is unresponsive to the scope of the search set forth in the warrant. Compare Exhibit 5 with Exhibit F. Categorically exempting the viewing of nonresponsive evidence pursuant to the plain view doctrine intrudes to too great of a degree upon an individual's privacy and is not needed to promote legitimate government interests. Riley, 134 S. Ct. at 2484. Agents can, with little additional burden, obtain a second search warrant instead. Accordingly, this court recommends the plain view exception to the warrant requirement be held not applicable in searches of digital evidence.

2. Even If Plain View is Theoretically Applicable, It Does Not Apply Here

Despite the sound and important reasons grounded in the Fourth Amendment for not applying the plain view doctrine to digital searches, some courts have applied the plain view doctrine to examinations of digital data pursuant to a search warrant authorizing a search for one kind of evidence, where the police discover evidence of another crime. See e.g. United States v. Mann, 592 F.3d 779, 784-85 (7th Cir. 2010); United States v. Williams, 592 F.3d 511, 521-22 (4th Cir. 2010).[5] However, this case is distinguishable from these cases applying the plain view doctrine: Agent Fair did not discover the evidence on Mr. Hulscher's cell phone while looking for evidence of forgery and counterfeiting pursuant to a valid search warrant for those items. Nor did the Det. Spinsby, who executed the forgery warrant, note any obviously incriminating evidence as to firearms offenses. Instead, Agent Fair seized digital data which a state court had authorized state police to search for evidence of forgery and counterfeiting, and he, a federal agent, began to search specifically for evidence related to Mr. Hulscher's federal firearms charges. Thus, Agent Fair was not acting pursuant to the initial warrant and attempting to search within the scope of that warrant when he inadvertently came across evidence of firearms offenses. Instead, from the inception of Agent Fair's receipt of the digital copy of Mr. Hulscher's phone, he had a different purpose

[5] The plain view holding in Williams was an alternative holding. The court also alternatively held that the evidence discovered on Williams' computer was within the scope of the evidence described with particularity in the search warrant. Williams, 592 F.3d at 519-21.

for his search.[6] This court has found no decision applying the plain view doctrine to facts such as are presented herein: (1) where the purpose of the second search was unrelated to the scope of the search warrant; (2) where the second search proceeded without a warrant; (3) where the second searcher is a person entirely different from the first person who lawfully searched pursuant to the warrant; and (4) where the first person who lawfully searched pursuant to the warrant did not take note of the evidence the second searcher looked for and now seeks to use at trial.

The plain view doctrine, even if it has general application in the context of searches of digital data, does not apply to Agent Fair's circumstances. Horton, 496 U.S. at 135; Morgan, 842 F.3d at 1075 (both holding officer must be in a lawful position to view the evidence). Also, the incriminating nature of the evidence must have been immediately apparent for the plain view doctrine to apply. Horton, 496 U.S. at 142; Khabeer, 410 F.3d at 482. The government has not shown this prong of the plain view test; if the incriminating nature of the evidence was immediately apparent, Det. Spinsby would have noted the evidence in his report (he did so as to drug trafficking evidence, but not firearms offenses). That Det. Spinsby did not note the evidence Agent Fair now seeks to use defeats the second element of the plain

[6] Tellingly, in asserting the plain view doctrine, the government argues *only* that Det. Spinsby was in a position to view the evidence in plain view. See Docket No. 232 at 11. The government's argument is in line with the case law: plain view would only apply to the officer who was lawfully executing the Huron search warrant, here, Det. Spinsby. Plain view would not apply to subsequent searchers of the property long after the initial lawful search was completed. This is especially true where, as here, Det. Spinsby noted no evidence of firearms violations in his lawful search.

view test. Finally, because Agent Fair did not obtain a search warrant as required under Riley, he did not have a lawful right to access the evidence, the third prong of the plain view showing. Khabeer, 410 F.3d at 482. It is the government's burden to show that plain view, an exception to the warrant requirement, applies. Coolidge, 403 U.S. at 443; Kennedy, 427 F.3d at 1140. They have failed to demonstrate their case by a preponderance of the evidence.

The conclusion is inescapable: Agent Fair should have applied for and obtained a second warrant which would have authorized him to search Mr. Hulscher's cell phone data for evidence of firearms offenses. Riley, 134 S. Ct. at 2485 (must have a search warrant to search a cell phone); CDT, 621 F.3d 1162, 1170-71, 1176 (plain view doctrine does not apply to nonresponsive digital data which is overseized by police); Carey, 172 F.3d at 1272-74 (plain view does not apply where officer is no longer pursuing search of items described in search warrant, but is avowedly searching for different evidence). Obtaining a second warrant would have been effortless—the digital evidence was already in the possession of police, so there was no risk that Mr. Hulscher would destroy or hide the evidence. The government had already obtained two indictments (now three), against Mr. Hulscher, so presumably it could show probable cause. And finally, the showing that evidence of firearms offenses might be on Mr. Hulscher's cell phone is also easy to make since, as the Riley Court noted, our cell phones reflect nearly everything about our daily lives.

In United States v. Johnston, 789 F.3d 934, 942-43 (9th Cir. 2015), the Ninth Circuit upheld searches that occurred on defendant's mirror image hard

drive five years after the mirror images were initially created because the subsequent searches were squarely within the scope of the original search warrant and conducted by the same investigators to which the search warrant had been given for the same purpose. Id. The agent "was not digging around in unrelated files or locations that might have prompted the need for a second warrant." Id. at 942. Here, Agent Fair was "digging around in unrelated files or locations" looking for evidence not specified in the original search warrant. The reason the Ganias court upheld the search in that case was *because* the agent had obtained a second search warrant to cover her separate purpose for searching and then relied in good faith on the judge's issuance of that warrant. Ganias, 824 F.3d at 220-25.

Finally, this court notes that in this case, the criminal prosecution for which the original search warrant had been issued was completed at the time Agent Fair conducted his search. Mr. Hulscher had entered a plea and been sentenced on the theft/forgery/counterfeiting charges for which the original search warrant issued. In addition, the state court in that prosecution had ordered the police to return Mr. Hulscher's cell phone to him. Thus, it is questionable whether the Huron police were within the Constitution in keeping the digital copy of the phone's contents.

In Ganias, unlike this case, it was important to the court that Ganias had never made any request for the return of his personal financial information originally seized. Ganias, 824 F.3d at 207. Also, in Ganias the agents testified that for technology-related issues, they did not want to purge or segregate the

nonresponsive data from the data responsive to the two clients which were originally being investigated. Id. at 206. Here, Det. Spinsby apparently had no such concerns as the evidence presented to this court shows he *did* segregate the data responsive to his search warrant and save it separately from the digital copy of everything on Mr. Hulscher's phone. Compare Exhibit 5 with Exhibit F. However, like the Ganias court, this court refrains from deciding the issue whether the mere retention by the Huron Police Department of the copy of the data from his phone was a Fourth Amendment violation. But even if that retention was constitutional, it clearly was a Fourth Amendment violation for Agent Fair to obtain and search the digital data from the Huron police under these circumstances.

The court holds the plain view doctrine has no application in searches of nonresponsive digital evidence. Alternatively, if the plain view doctrine applies to such searches generally, it does not apply under these circumstances because Agent Fair was not lawfully at the vantage point from which he saw the evidence, the incriminating nature of the evidence was not immediately apparent, and Agent Fair did not have lawful access to seize the data at the time he saw it.

The government argued orally that law enforcement agencies are free to share information among themselves and are not required to purge the evidence in their possession once a case is completed. The court takes no quarrel with that assertion at all. It was not unlawful for the Huron Police Department to agree to make its evidence available to the ATF (assuming it was

lawful to retain it in the first place). But that begs the question whether it was incumbent upon the ATF to secure a search warrant before searching the data voluntarily given to it. The court concludes it was.

D. Exclusionary Rule

Even though the court has concluded that Agent Fair should have obtained a search warrant under these circumstances and that he did not do so, the application of the exclusionary rule is not automatic. The Supreme Court has stated that the mere fact of a Fourth Amendment violation does not dictate exclusion. Herring v. United States, 555 U.S. 135, 141 (2009). Rather, the exclusionary rule should be applied only where to do so will appreciably deter conduct which violates the Fourth Amendment. Id. (quoting Leon, 468 U.S. at 909). Courts should focus on whether excluding the evidence will efficaciously deter Fourth Amendment violations in the future. Id. (citing United States v. Calandra, 414 U.S. 338, 347-55 (1974)).

In addition, courts must determine if the benefits of deterrence outweigh the costs. Id. The primary cost of applying the exclusionary rule is the possibility that a guilty person may go free. Id. The benefit is the protection of the Constitution and holding law enforcement officers accountable. For the exclusionary rule to apply, the deterrent effect of exclusion must be substantial and outweigh any harm to the justice system. Id. at 147.

The Court has held the exclusionary rule inapplicable where the police violated the Fourth Amendment through negligence, where the police acted in objectively good faith reliance on a search warrant lacking in probable cause,

where police acted in good faith reliance on a search warrant that was invalid due to clerical error, to warrantless administrative searches pursuant to a statute later declared invalid, and to police who relied upon a court's computer database that mistakenly indicated an arrest warrant was outstanding. Id. at 142-43. In Herring, the court extended the computer database mistake to circumstances where the police maintained the database and negligently made a mistake rather than the judiciary. Id. at 146-48.

The cases where the Court applied the exclusionary rule usually involved intentional or flagrant violation of the Fourth Amendment. Id. at 143-44. For example, the rule was applied when police broke into a suspect's house without a warrant and took documents, and then returned later with United States Marshals to take more documents, under circumstances where no probable cause existed and no warrant would have issued had they applied for one. Id. (discussing Weeks v. United States, 232 U.S. 383, 393-94 (1914); and Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391 (1920)). In another case, the exclusionary rule was applied where police forced open a door to a house, kept the homeowner's lawyer from entering, brandished a false warrant, handcuffed the woman and proceeded to search the entire house. Herring, 555 U.S. at 144 (discussing Mapp v. Ohio, 367 U.S. 643, 644-45 (1961)).

Distinguishing the cases where the exclusionary rule was applied from those where it was not, the Court held police conduct "must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable

that such deterrence is worth the price paid by the justice system." Id. The conduct must be reckless, deliberate, grossly negligent, or recurring/systemic negligence. Id. Furthermore, the inquiry into deterrence and culpability is an objective one—it is not based on the actual officer's subjective awareness of the nature of his conduct. Id. at 145.

Here, Agent Fair's conduct transgressed some bright-line rules of the Fourth Amendment. Cell phone searches require search warrants unless there are special circumstances. Riley, 134 S. Ct. at 2493. Searches pursuant to a search warrant are limited to the scope of the search and the things described with particularity in the search warrant. Andresen, 427 U.S. at 480. The plain view exception only applies if the police observe something in plain view from a lawful vantage point and the incriminating nature of the evidence is patent. Horton, 496 U.S. at 142; Khabeer, 410 F.3d at 482; Morgan, 842 F.3d at 1075. A reasonable, ordinary law enforcement agent (the test is an objective one), would know this. Accordingly, the police conduct here is sufficiently deliberate so that exclusion will have a meaningful and substantial deterrent effect.[7]

What risks are presented to the judicial system if the evidence from the digital data extracted from Mr. Hulscher's phone is excluded? This case has been set for trial six times, all but two of those trial dates predating January

[7] Although this does not enter into the court's analysis, it notes anecdotally that this court routinely receives search warrant requests from local ATF agents seeking to search cell phones that were previously seized by city or county law enforcement in connection with a state crime and are relevant to some separate federal investigation. The notion that Agent Fair should have obtained a search warrant here is not novel.

18, 2017.[8] On these dates prior to Agent Fair's discovery of the evidence at issue in this motion, the government represented it was ready, willing and able to go to trial. In other words, the government was confident it could prove its case against Mr. Hulscher beyond a reasonable doubt without the evidence. This weighs in favor of suppressing. Furthermore, the evidence the government has identified as wanting to use from the digital copy of Mr. Hulscher's phone appears to be peripheral in nature—it is not direct evidence of the firearms offenses with which he is charged. This too mitigates in favor of exclusion. Finally, because of the routine overseizure of digital/electronic evidence by law enforcement, and the vast amount of and highly personal nature of nonresponsive data in each of those overseizures, the threat to the continuing validity of the Fourth Amendment's prohibition against general warrants also favors exclusion. Accordingly, because the deterrent effect is substantial and the costs to the justice system are not, this court recommends application of the exclusionary rule.

---

[8] The trial in this case was first set for September 27, 2016, and was reset to November 1, 2016, after a motion to continue was filed by Mr. Hulscher. See Docket Nos. 59, 73, & 79. Next, two co-defendants moved to continue and the jury trial was reset for December 20, 2016. See Docket Nos. 86, 88 & 90. The government then moved to continue this trial date in order to have more time to address various pending motions by the defendants. See Docket No. 117. Trial was set for January 3, 2017. See Docket No. 120. The government again moved to continue, but the district court denied the request. See Docket Nos. 121 & 124. A co-defendant moved to continue the trial on January 3, 2017, after the government revealed new evidence on the eve of trial and trial was reset for January 24, 2017. See Docket No. 172. The government moved to continue this date on January 20, because it had by this time discovered the Huron evidence and Det. Spinsby was unavailable to testify the week of January 24. See Docket No. 204. The jury trial was then set for its current date of February 22, 2017. See Docket No. 210.

CONCLUSION

Based on the foregoing law, facts, and analysis, this magistrate judge respectfully recommends granting defendant Robert John Hulscher's motion to suppress [Docket No. 223] the evidence Agent Fair obtained from his warrantless search of the digital data from Mr. Hulscher's cell phone.

NOTICE OF RIGHT TO APPEAL

The parties have stipulated to limit their time to appeal to this report and recommendation in order to maintain their current jury trial start date. Accordingly, pursuant to that stipulation, the parties have three (3) days after service of this report and recommendation to file written objections pursuant to 28 U.S.C. § 636(b)(1)(B), unless an extension of time for good cause is obtained. See FED. R. CRIM. P. 59(b); 28 U.S.C. § 636(b)(1)(B). Failure to file timely file objections will result in the waiver of the right to appeal questions of fact. Id. Objections must be timely and specific in order to require *de novo* review by the district court. See Thompson v. Nix, 897 F.2d 356 (8th Cir. 1990); Nash v. Black, 781 F.2d 665 (8th Cir. 1986).

Objections are due by 12:00 midnight on Wednesday, February 15, 2017.

DATED February 10, 2017.

BY THE COURT:

VERONICA L. DUFFY
United States Magistrate Judge